Analiza bezpieczeństwa wybranych narzędzi informatycznych

Liczba stron: 119

Nazwa Szkoły Wyższej: AKADEMIA EKONOMICZNA W Katowicach

Rodzaj pracy: magisterska

Rok oddania: 2008

Spis treści

Wstęp

Tematem niniejszej pracy jest problematyka bezpieczeństwa narzędzi informatycznych służących do komunikacji we współczesnym społeczeństwie informacyjnym. Dzięki Internetowi cały świat stał się jedną wielką „globalną wioską". Codziennie tysiące użytkowników sieci, wymienia miliardy informacji. Praktycznie nie ma Internauty, który nie posługiwałby się pocztą internetową oraz komunikatorami. Narzędzia te, w ostatnich latach zaczęto wykorzystywać na masową skale co doprowadziło, że stały się podstawowymi narzędziami pracy wielu ludzi. Jednak niewielki procent ich użytkowników ma świadomość niebezpieczeństw jakie pociąga za sobą ich użytkowanie.

Użytkownicy tych narzędzi korzystają z globalnej sieci komputerowej, jaką jest Internet. Jednak obecnie niesie ona ze sobą wiele zagrożeń. Dziś prócz wirusów mamy do czynienia m. in. z trojanami, robakami internetowymi, ze zjawiskiem podszywania się pod kogoś innego zarówno ze strony klienta jak i serwera, wykradania haseł i informacji oraz podsłuchiwaniem ruchu internetowego. O ile przeciętny użytkownik sieci ma świadomość, że powinien zainstalować program

antywirusowy z aktualną bazą wirusów w komputerze, aby zwiększyć poziom bezpieczeństwa swoich danych, o tyle świadomość istnienia zjawisk takich jak podsłuchiwanie transmisji oraz możliwość podszywania się pod kogoś nie jest już taka oczywista.

Dlatego też celem poznawczym niniejszej pracy będzie analiza protokołów i mechanizmów w sieciach komputerowych z punktu widzenia bezpieczeństwa. Dokładniej zostanie przedstawione bezpieczeństwo komunikatorów internetowych rozpoczynając od pierwszego narzędzia, które umożliwiało komunikacje – „IRC". Kolejno protoplastę wszystkich komunikatorów jakie są znane aktualnie – „ICQ". Następnie komunikatory doskonale znane na polskim rynku, takie jak „Gadu-Gadu" oraz „Jabber". Zostaną zbadane też protokoły przesyłania poczty internetowej oraz sposoby jej zabezpieczania. Techniki zabezpieczania połączeń z serwerami, metody zabezpieczania treści wiadomości jak i mechanizm uwierzytelniania tożsamości nadawcy, czyli podpisu cyfrowego. Dodatkowo przedstawione zostaną najpopularniejsze metody przechowywania poczty na serwerach.

Natomiast celem utylitarnym pracy będzie, opracowanie raportu prezentującego słabość bezpieczeństwa popularnych narzędzi informatycznych w kontekście tajności przesyłanych danych. W raporcie tym uwzględnione zostanie bezpieczeństwo w/w narzędzi informatycznych. Głównymi narzędziami, które zostaną wykorzystane do badania bezpieczeństwa będą „sniffery" oraz wszelkie inne narzędzia pomocne przy testowaniu bezpieczeństwa sieci.

Teza pracy stanowi, że domyślna konfiguracja współczesnych narzędzi informatycznych nie zapewnia odpowiedniego poziomu bezpieczeństwa danych, pomimo istnienia mechanizmów zabezpieczających.

W rozdziale pierwszym zostały przedstawione podstawy teoretyczne dotyczące sieci komputerowych.

Drugi rozdział to przedstawienie problematyki bezpieczeństwa informacji w sieciach komputerowych, połączeń szyfrowanych oraz podpisów cyfrowych.

W rozdziale trzecim przeanalizowane zostały popularne narzędzia pozwalające na komunikowanie się w sieci, takie jak IRC, ICQ, Gadu-Gadu i Jabber.

W ostatnim rozdziale przedstawiono narzędzia sprawdzające bezpieczeństwo,

zbadano tajność komunikatorów internetowych oraz sprawdzono w jakim stopniu wykorzystywana jest technologia aby zwiększyć bezpieczeństwo poczty internetowej.

To jest gotowa, obroniona praca. Gdyby chcieli Państwo zlecić napisanie zupełnie nowej pracy, to zapraszamy na stronę pisanie prac - sprawdzony serwis!